Maciej Palmowski - How we closed almost 1000 plugins in a month

[00:01:21.320]
Hello Page Builder Summit. Really glad to be here with you. And today I'm going to share a very interesting story. A story of how we were able to remove almost 1000 plugins during one month from the official WordPress repository. My name is Maciej Palmowski, I work at Patchstack.

[00:01:43.510]
I hope you already know this company. We take care of open source security, WordPress included. So if you didn't heard about us yet, you should really Google PatchStack and read a bit about us. I work as a security community manager.

[00:02:03.260]
First we need to answer this question because we are at Page Builder Summit, right? So we are at a conference where we are talking about how to build websites, how to build faster, better and here and here we we have Maciej Palmowski from PatchStack talking about some about removing thousands of plugins. Who cares, right? Well you should, you should. Because while building website is one thing, probably also want to maintain those websites to each month earn some money from the client for which you build the website.

[00:02:42.830]
And security is one of the things you should be taking care of. And the thing that we did show some things about how security in WordPress

works, about which things you should be extra careful about and what works really well. So that's why you should care. I will start with a very unpopular opinion. In my opinion WordPress is very secure.

[00:03:18.260]
I'm really not kidding, I'm dead serious here. So we are talking about the CMS that has over 40% of the market. So it's a dream of every bad hacker to find a vulnerability inside. Because you know, finding such a vulnerability would gave this person access to well, 30% of the Internet, right? But the truth is that last year we only found seven vulnerabilities inside of WordPress.

[00:03:53.770]
Year earlier it was also seven and none of them were severe. So really WordPress is very secure. I would be, I can even tell WordPress is the most secure open source CMS on the market if you don't use any plugin. And that's the problem because let's be honest, that's one of the reasons why we are using WordPress because of its ecosystem. WordPress ecosystem is amazing.

[00:04:25.560]
It's huge. It lets you extend WordPress to whatever you want with a few clicks. Sadly, it's also the main reason of WordPress problems. Let's take a look at some numbers.

[00:04:43.010]
So, 96% of the vulnerabilities we found. And by we, I don't mean just PatchStack, but all of us. So we are talking about PatchStack, we are talking about Wordfence, we are talking about WPScan were found in plugins and we are talking about more than seven and a half thousand vulnerabilities found. To compare, we only found 326 vulnerabilities inside of themes and those seven in core.

[00:05:21.510]
Also, if we look how it changed over the years, we can see that in 2022 all of us were only able to find 4,000 vulnerabilities. In 2024 we were able to find almost 8,000, so twice as much. Also, as you can see based on the colours here, the amount of critical vulnerability is also higher than it

was. And while it might look scary, the truth is that's good news that we are finding those things because if we can find them, we can inform the author and author can fix it. And in most cases they do.

[00:06:07.330]
So every time when we are finding a vulnerability, we can start the whole process of fixing it after releasing an update. And at some point you will see this possibility to update the plugin inside of your WP app. Like I said, that's great.

[00:06:28.040]
So I mentioned that we found those that we're able to close this thousand, almost thousand plugins from the official WordPress repository. Yeah, you know this, right? You are probably using it every day.

[00:06:47.410]
Let's remember that official repository holds over 60,000 plugins, which is quite a lot. Everyone after initial review can add a plugin, right? So every time when you submit the plugin, you go through the initial review and if everything is okay, your plugin is published there, but it's not reviewed later. So every time when you update your plugin, it won't be reviewed anymore. So if you were able to push good code during your initial review, that's perfect.

[00:07:27.160]
But if you introduce a vulnerability during your first update, you won't be noticed, at least not by the reviews. At Patchstack we have our regular bug bounty programme. So every month hackers, but by hackers this time I mean those good ones, we should even call them security researchers. So they're finding and reporting vulnerabilities to us for this. They get experience points. Based on the amount of those experience points, they they take some place in the leaderboard and based on their position, they earn money.

[00:08:17.740]
And this process repeats over and over and over.

[00:08:23.340]
Back then, our bug bounty programme, and if I remember, not only ours, it was quite, quite common, had some limitations. First of all, if you wanted to report something, this plugin or theme had to have over 1000 instals. On the other hand, it had to be updated in the last three years. So our rules back then made it impossible to report either old plugins or plugins that were that never got popular.

[00:09:04.930]
And in October, because October is Cyber Security Month, we decided to launch a special event because we are doing those special events to to make our mountain bug bounty a bit more interesting from time to time. So we decided to do this colossal cleanup. And our plan was simple. We removed two rules. First of all, every plugin that had less than thousand instals were treated as it would have thousand instals.

[00:09:41.420]
Also, we removed the limitation of three years since last update. And there was just one catch. Those exceptions applied only for reports with a CVSS score of 65 or more. And that's it. On first October we started the event.

[00:10:03.880]
Of course we started with a typical discord announcement. So we informed that we are changing those rules and yeah, we were hoping for the best. On 4th of October we already got 90 reports.

[00:10:23.090]
Just to give you some scale, our record back then was If I remember, 626reports, if I'm correct, during one month. So while this number looks promising, we are always extra careful about those reports that are happening at the beginning, at and at the end of the month because sometimes some researchers are kind of holding some reports based on the situation in the leaderboard. So those reports weren't anything special at the same time. Yeah, we know it was after WordCamp US. So this WordPress drama kept on drumming and we were a bit afraid that it will affect the researchers that they will be a bit distracted. After first week we already had 123 reports.

[00:11:25.440]
So you can see that that it wasn't growing as quickly as after the first four days. But we were hoping that we will reach around 500. Week later we already had 352 reports. So at this point we were really counting that we will beat our previous record. We saw that 700 is in reach and 16 October was one of the most pivotal moments of the event. Why?

[00:12:06.160]
Because this was the moment when some of the researchers announced that they finally downloaded all the plugins to their drive, to their hard drives. Why? It's important because security researchers don't just pick a plugin, check the check its code and if they don't find anything, they pick another one. No, it doesn't work that way. They try to find a pattern and if they find a pattern, then they try to apply the same pattern to as many other plugins as possible.

[00:12:43.070]
So because of the limitation back then, let me remind you, 1,000 instals or more, everyone had underdrives. All the plugins with more than thousand installs, they didn't had those that had from 0 to 999. So they had to download. And what's interesting, most plugins in the official WordPress repository has less than 1,000 instals. It was kind of a shock for me.

[00:13:21.580]
But yeah, so yeah, around half of the amount researchers had all the plugins of their drives and we started seeing this in the amount of reports that started to happen.

[00:13:37.500]
But we also decided to make it a bit more spicy. So on the 16th of October we also announced that if all together they will find 1000 reports or more, everyone who reported at least 10 reports will get an extra $100 bounty. So half of a month to go. 487 reports. So it was about 32 reports per day and we were seeing that two days later it was only 31 reports a day needed.

[00:14:21.730]
Around the third week the amount of reports was changing so quickly. Like this wasn't a joke. Someone from our team posted on Twitter that hey, we have 600 reports. When I saw this tweet and I refreshed the leaderboard, I already see that we have 679. So it was growing that quickly.

[00:14:47.210]
On the 25th of October we cross that 1000 valid reports line. It was huge. So we already beat our record. And now it was now we were just waiting how many reports we will get. In the end on 29th we were, we already had 1240 and it was still going.

[00:15:22.030]
On 21st of October, Enrique Chavez saw something interesting because he's monitoring the official repository and he saw that around 1000 plugins is gone from the official repository.

[00:15:40.110]
At this point many people thought that it's connected with everything that is happening after WordCamp US. Positive. But no, it was us.

[00:15:54.120]
On 4th of November, we were still waiting to review the last four reports. Stealthcopter was leading by one point over Kinorth. And what were the consequences? Well, first of all, 946 plugins got removed from the official repository and that's great because they were both vulnerable and in most cases just abandoned. So using them was a serious security threat.

[00:16:28.510]
So that's great.

[00:16:33.250]
There is a problem. Many users won't even learn about this because WordPress has this amazing system that helps you always know that a plugin requires an update. It's really amazing, right? You just log into your WP admin and you see this bar saying that hey, press here to update your plugin. It's really amazing, but I don't know why, but we

don't have a similar thing that would inform you about hey, you shouldn't use this plugin, it's closed because of security reasons.

[00:17:12.550]
And while for a moment it seemed that something like this will show up in Core, well, it won't.

[00:17:27.750]
This event also surprised us because we weren't expecting that we'll get that many reports that will be able to remove so much plugins. That's why we decided to change our rules a bit to make it easier for plugins with lower instal count and for plugins that weren't updated lately also to be reported.

[00:18:01.710]
And during this event we found some really interesting vulnerabilities. For example, you could log in just by adding ID equals 1 or ID equals ID of the admin. Very simple, right? Or it was in registration endpoint and if the username was already taken it just logged you in. Amazing.

[00:18:31.480]
Normally you should get an error, but this approach was a bit different Also a month after our event Warfence did a similar event. If I recall, they got over 700 reports. They didn't share how many plugins they closed, but it doesn't matter. Those two events together made WordPress safer, the WordPress repository safest ever also. Yeah, those are all the heroes who reported at least one vulnerability during this epic event.

[00:19:21.010]
Really they all those people are amazing. Also huge thanks to WordPress reviews team because they also had a very difficult month because they were constantly having to respond to our emails and of course to our team, to Darius, to Rafi, to Ananda, to Kushat, to Chas, and to Edward because well, it was a very difficult month for them with the flood of reports but they managed, they managed to validate all of it and here we are today. So WordPress got safer but like I mentioned, users aren't notified about those closures which is a huge problem and this really should change. Also I think that security researcher work still isn't seen

as WordPress contribution, which is also a mistake because we are all in this together. Some of us are building things and some of us are looking at this code and finding mistakes, vulnerabilities and working together and only by working together, we will have a healthy ecosystem.

[00:20:59.900]
That's why I really think that security research at work should be seen as a normal WordPress contribution.

[00:21:08.380]
Also, it's quite obvious to see that we need a better review mechanism because the current one, well, just isn't working.

[00:21:22.380]
And I want to say that both security and Reviews Themes in WordPress are amazing. They're doing a lot of great and hard work. But the truth is that they are too small and underfounded and they can only in most cases do reactive work. So if you are thinking about how you can invest in WordPress ecosystem, think about sponsoring some someone from the security or review teams. It will be really money well spent.

[00:22:04.230]
Okay, so what you should remember from my talk. First of all, take security seriously. Because if you won't take for example SEO seriously, well, your website will be ranked a bit lower, but you can always recover. If you won't take performance seriously, the website will be working slower. You might lose some clients, but again, you can fix it quickly. If you don't take security seriously, you may lose everything.

[00:22:47.540]
So remember, always take security seriously. Also remember that installing a plugin from the official repository doesn't guarantee that it's secure. Installing from any other marketplace also doesn't guarantee that it's secure. Just remember it. And every time when you instal something, do some research.

[00:23:11.070]

There are databases, for example Patchstack has one. When you can see a history of the plugin, you can see how many vulnerabilities it had over time. How did they react to those vulnerabilities? How quickly they were fake. Those vulnerabilities were fixed.

[00:23:28.140]
So do some research and let me repeat myself. Take security seriously. It's not a task, it's a constant, ongoing process. You won't fix it with just one click. With installing a plugin, it will always be there.

[00:23:51.260]
So thank you. I hope you enjoyed my talk and if you did, apart from of course visiting Patchstack website, don't forget to subscribe to my newsletter. I very often post some news about WordPress, about security and about many, many other things. So thank you. It has been a pleasure being here again and well, see you next time.

[00:24:18.760]
Bye.